ALIBABA CLOUD

阿里云

数据库审计
快速入门

文档版本：20201029

阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
Courier字体	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1.C100快速入门

本文介绍了开通C100数据库审计实例后，通过配置向导快速部署和使用数据库审计服务的具体操作。

前提条件

已开通C100数据库审计实例。

背景信息

数据库审计系统支持对ECS自建数据库和RDS云数据库进行审计。

- ECS自建数据库

  对于在ECS云服务器上自建的数据库，数据库审计系统支持国内外各类主流数据库，具体支持的数据库版本请参见下表。

数据库	版本
Oracle	8i、9i、10g、11g、12c、18c、19c
MySQL	4.0、4.1、5.0、5.1、5.5、5.6、5.7、8.0
SQL Server	2000、2005、2008、2012、2014、2016、2017
Sybase	11.9、12.5
DB2	V80、V81、V82、V95
Informix	IDS 9
Oscar	5.5、5.7
达梦（DM）	DM7
Cache	所有版本
PostgreSQL	9、10、11
DCOM	所有版本
Teradata	所有版本
人大金仓（Kingbase）	V6
GBase	8.5a、8.8s
MariaDB	5.1、5.2、5.3、5.5、10.0、10.1、10.2、10.3
WEB	所有版本
FTP	所有版本
SMTP	所有版本

数据库	版本
POP3	所有版本
Hana	1
MongoDB	2.x、3.x、4.x
HBase (protobuf)	所有版本
HBase (thrift)	thrift1、thrift2
Hive	所有版本
Redis	所有版本
Elasticsearch	所有版本
Cassandra	3.X
HDFS	所有版本
Impala	3.X
GaussDB	100、200、300

- RDS云数据库

  对于RDS云数据库，数据库审计系统支持的版本情况请参见以下表格。

数据库	版本
MySQL	5.5、5.6、5.7、8.0
SQL Server	2008、2012、2016、2017
PostgreSQL	9、10、11
MariaDB	10.3

操作步骤

1. 登录云盾数据库审计系统。具体操作请参见登录数据库审计系统。
2. 添加要审计的数据库。
   i. 在**资产 > 资产管理**页面，单击**新增**。
   ii. 在**新增资产**页面，完成数据库配置。

   推荐您添加RDS型数据库，您可以直接从当前阿里云账号下已开通的RDS实例中选择要添加的实例。

   您也可以添加ECS自建数据库，具体配置描述请参见ECS自建数据库配置。

   

   iii. 单击**保存**。

3. 安装流量采集工具（Agent）。

   如果数据库服务器是安装了云助手的Linux系统ECS，推荐您通过云助手安装Agent；否则，您需要根据数据库服务器的操作系统类型，下载相应的Agent并手动安装。以下步骤描述了通过云助手安装Agent的方法，关于手动安装Agent，请参见部署Agent程序。

   i. 在**系统管理 > Agent管理 > Agent安装**页面，单击**开始安装**。

   ii. 在**通过云助手安装Agent**对话框，定位到要安装Agent的实例。

   iii. 单击实例操作列下的**安装**。
   等待Agent安装完成。安装完成后，**Agent状态**显示为**运行中，已连接**。

4. 配置审计规则。具体操作请参见为数据库配置审计规则。

   审计规则帮助您发现数据库中的风险。为数据库配置审计规则后，当审计记录命中规则时，会触发告警。

5. 配置告警通知。

   i. 在左侧导航栏，单击**资产 > 资产管理 > 资产列表**。

   ii. 在需要配置告警通知的资产所在行，单击**操作**列的**管理**。进入资产管理详情页面。

   iii. 在左侧导航栏，单击**告警通知**。

   iv. 根据需要的告警通知形式，在**短信通知**或**邮件通知**页签单击**新增**。

   v. 在**新增告警通知配置**页面，完成告警通知配置。

参数	说明
接收者	新增短信通知时，配置告警接收人的手机号码。新增邮件通知时，配置告警接收人的邮件地址。
告警等级	设置告警的严重等级，支持*低*、*中*和*高*。
告警次数限制	表示24小时内触发同一规则最多发送的告警次数上限，有效范围0~9999。 每天零点告警计数清零。 当该项设置为0时，不会发送告警通知。

   vi. 单击**保存**。
   配置成功后，当有告警生成，您配置的接收方式会收到告警通知。

6. 订阅报表。

   添加订阅报表任务后，数据库审计系统会定期向您指定的邮箱发送订阅的数据库审计报表，帮助您了解数据库状态。请参见以下步骤，创建订阅任务。

   i. 在**报表中心 > 报表订阅**页面，单击**添加**。

ii. 在**添加订阅任务**页面，完成订阅任务配置。订阅任务配置描述请参见订阅任务配置描述。

iii. 单击**保存**。
成功添加订阅任务。

2.A100快速入门

购买A100数据库审计实例后，您需要登录数据库审计系统完成数据库接入操作，并在数据库服务器上部署Agent程序，才能为您的数据库启用审计服务。

支持审计的数据库

数据库审计系统支持对ECS云服务器自建数据库和RDS云数据库实例进行审计。

- ECS自建数据库

  对于在ECS云服务器上自建的数据库，数据库审计系统支持国内外各类主流数据库，具体参见下表说明。

数据库类型	支持的版本
Oracle	Oracle 9i、10g、11g、12C
SQL Server	SQL Server 2005、2008、2012、2014
MySQL	MySQL 4.0、4.1、5.0~5.7、8.0
DB2	DB2 8.1、8.2、9.1、9.5、9.7、10.1
SAP HANA	SAP HANA 1.0、2.0
PostgreSQL	所有版本
达梦（DM）	DM 6、7
人大金仓（KingBase）	KingBase 7及以上
南大通用（GBase）	GBase 8、GBase 8T
Sybase	Sybase 12、15
神通数据库（Oscar）	不限

- RDS云数据库

  对于RDS云数据库，数据库审计系统支持情况参见下表说明。

数据库类型	支持的版本
MySQL	MySQL 5.5、5.6、5.7、8.0
SQL Server	SQL Server 2008 R2、2012、2016、2017
PostgreSQL	所有版本
MariaDB	MariaDB 10.3
PPAS	PPAS 9.3、10

关联应用

数据库审计系统支持以下关联应用类型：

应用	支持的版本
Tomcat	Tomcat 5.5、6.0、7.0、8.0 **说明** 对于Tomcat 5.5版本，需要安装JRE 1.6或以上版本。
JBoss	JBoss 4、5 **说明** 对于JBoss 4版本，需要安装JRE 1.6或以上版本。
WebLogic	WebLogic 10、11
WebSphere	WebSphere 6.1、7、8 **说明** 对于WebSphere 6.1版本，需要安装JDK 1.6或以上版本。

使用流程

开通A100数据库审计实例后，您需要完成以下任务，为数据库启用审计服务并查询审计结果。有关开通实例的详细内容请参见开通数据库审计实例。

任务	描述
步骤1：启用数据库审计实例	开通数据库实例后后，您必须启用实例，才能登录数据库审计系统并使用审计服务。
步骤2：管理数据库审计实例	启用数据库审计实例后，您可以调整实例的安全组和内外网访问控制策略。 **说明** 初次使用时建议您保留默认值，待完全熟悉服务后再做调试。
步骤3：登录数据库审计系统	登录数据库审计系统后，您可以在系统中完成数据库接入配置和查询审计结果。
步骤4：添加数据库实例	在数据库审计系统中添加需要审计的数据库实例的相关信息。
步骤5：部署Agent程序	在数据库审计系统中添加数据库实例后，您必须在数据库服务器上部署Agent程序，才能使数据库审计服务收集目标数据库的访问流量信息，并进行审计。
步骤6：查看系统审计结果	完成数据库接入和Agent部署后，您可以在数据库审计系统查看审计到的语句和统计信息。